EXHIBIT A

COMPLAINT

STATE OF VERMONT

SUPERIOR COURT
Chittenden Unit

CIVIL DIVISION
Docket No. _____

_____X

DAVID MORGAN, on behalf of himself and all others similarly situated,

Plaintiff

v.

THE BURTON CORPORATION d/b/a BURTON SNOWBOARDS

Defendant

_____X

CLASS ACTION COMPLAINT

Plaintiff, DAVID MORGAN (hereinafter, "Plaintiff"), on behalf of himself, and all others similarly situated, for his causes of action against the Defendant, THE BURTON CORPORATION D/B/A BURTON SNOWBOARDS ("Defendant" or "Burton"), alleges upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This action arises out of Defendant's unauthorized disclosure of the confidential personal information, Personally Identifying Information[1] ("PII"), of Plaintiff and the proposed Class Members, over 5,000 individuals, beginning on February 11, 2023 during a cyberattack on

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

Burton's systems, including their names, dates of birth, Social Security numbers, driver's license numbers or state issued identification number, passport number, and financial account information (the "Data Breach").[2]

2. Founded in 1977, Burton is a privately owned company based in Burlington, Vermont which manufactures and sells snowboards and other recreational equipment, accessories, and apparel,[3] and the second largest snowboard manufacturer in the United States.

3. According to Burton, it collects data from The Chill Foundation, a Vermont non-profit corporation on Burton's campus,[4] which "inspires young people through boardsports and builds a more equitable outdoor community,"[5] including from Chill's employees.

4. Further, on information and belief, Burton collects massive amounts of PII of its employees and prospective employees, including Plaintiff and the Class Members, which it stores on its computer network systems.

5. On information and belief, Burton failed to undertake adequate measures to safeguard the PII of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity

---

[2] *See*: The Burton Corporation, Data Breach Notifications, Maine Attorney General, March 28, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/027f1a31-da35-49fe-a73f-10d0caeb5224.shtml (last acc. July 3, 2023);

The Burton Corporation, Data Breach Notification to Maine Attorney General, including sample Notice, March 27, 2023, **("March 27, 2023 Data Breach Notice") attached as Exhibit 1;**

The Burton Corporation, Data Breach Notifications, Maine Attorney General, May 26, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/74956a55-1020-4d9e-a3d6-0e9398870ebd.shtml (last acc. July 3, 2023);

The Burton Corporation, Data Breach Notification to Maine Attorney General, including sample Notice, May 26, 2023, **("May 26, 2023 Data Breach Notice") attached as Exhibit 2.**

[3] https://www.burton.com/us/en/about-us

[4] *See* March 27, 2023 Data Breach Notice, Exhibit 1.

[5] Chill website, available at https://www.chill.org/ (last accessed July 6, 2023).

protocols, resulting in the Data Breach.

6. Although Burton discovered the Data Breach on or about March 9, 2023, Defendant failed to notify and warn Data Breach victims of the unauthorized disclosure of their PII until March 27, 2023, and on information and belief, did not notify the majority of the proposed Class Members until May 26, 2023.

7. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive PII and fully warn them promptly and fully about the Data Breach, they have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

PARTIES

8. Plaintiff is a natural person, and resident and citizen of the State of California with a primary residence in Ventura, California, where he intends to remain, and a victim of Defendant's Data Breach.

9. Burton is a corporation organized and existing under the laws of the State of Vermont with a principal place of business located at 180 Queen City Park Road, Burlington, Vermont 05401.

JURISDICTION AND VENUE

10. This Court has personal jurisdiction over Defendant because, Burton maintains its principal place of business and headquarters in Vermont, and operates, conducts, engages in, or carries on a business in this state.

11. Jurisdiction is proper in this Court pursuant to 4 V.S.A. § 31.

12. Venue is proper in this Court pursuant to 12 V.S.A. §§ 402(a) as the unit where Defendant resides.

13. Class action certification is appropriate pursuant to Vermont Rules of Civil Procedure Rule 23.

FACTUAL BACKGROUND

A. Defendant Burton

14. Founded in 1977 as Burton Snowboards, Burton is a privately-held, global corporation headquartered in Burlington, Vermont, which designs, manufactures and sells snowboards, snowboarding tools, snowboard apparel, and other apparel and products.[6]

15. Burton maintains its global office in Burlington, Vermont, as well as a prototype facility, and offices in Australia, Austria, Canada, China, and Japan.[7]

16. As of 2018, Burton had over a thousand employees, and "an estimated $400 million in revenue and a 32% share of the global snowboarding market [and] is valued at approximately $700 million."[8]

17. Burton owns and operates flagship retail stores across the United States and the globe, at Burlington Headquarters in Burlington, Vermont; Stratton, Vermont; Denver, Colorado; Boulder, Colorado; Avon, Colorado; Telluride, Colorado; Vail Colorado; Winter Park, Colorado; New York, New York; Santa Monica, California; Truckee, California; Boston, Massachusetts; Park City, Utah; Wrentham, Massachusetts; Montreal, Quebec, Canada; Bromont, Quebec; Mont Tremblant, Quebec; Blue Mountains, Ontario; Toronto, Ontario; Big Sky, Montana; Breckenridge,

---

[6] The Burton Corporation website, avail. at https://www.burton.com/us/en/about-us (last accessed July 3, 2023).

[7] The Burton Corporation website, avail. at https://www.burton.com/us/en/content/working-at-burton.html (last accessed July 3, 2023).

[8] Elizabeth Brier, Forbes, No. 22, 2019, "The Final Interview With Snowboard King Jake Burton Carpenter," available at https://www.forbes.com/sites/elisabethbrier/2019/11/22/the-final-interview-with-snowboard-king-jake-burton-carpenter/?sh=82940b274a68 (last accessed July 3, 2023).

Colorado; Chicago, Illinois; Carrabassett Vly, Maine; Innsbruck, Austria; Stockholm, Sweden; Munich, Germany; Chorzów, Poland; Nové Město, Czech Republic; Soorts-Hossegor, France; Avoriaz, France; Zürich, Switzerland; Verbier, Switzerland; Lausanne, Switzerland; Helsinki, Finland, Laax, Switzerland; Escaldes Engordany, Andorra; Milan, Italy; Beijing, China; Tokyo, Japan; Sapporo, Japan; Yokohama, Japan; Niseko, Japan; Nagano, Japan; Osaka, Japan; Karuizawa, Japan; Rusutsu, Japan; Nagano, Japan; Skijam Katsuyama, Fukui, Japan; Queenstown, New Zealand; and in Thredbo , Australia 2625.[9]

18. The Chill Foundation ("Chill") is a non-profit Vermont corporation, an "intervention program,"[10] also located at Burton's headquarters at 180 Queen City Park Road, Burlington, Vermont.

19. On information and belief, Burton owns and operates Chill, and Donna G. Carpenter, Defendant's owner and Chair of the Board of Directors,[11] is President of Chill.[12]

20. Chill, founded in 1995 by Burton's founders, Jake Carpenter and Donna Carpenter, provides programs to marginalized youth, including "experiential learning activities, reflection, and discussion, paired with boardsport lessons." As Chill says, the non-profit "…strives to remove all barriers to accessing boardsports by providing youth with everything they need to get after it, at absolutely no cost. New skills gained through boardsport skills progression and core-value

---

[9] The Burton Corporation website, avail. at https://www.burton.com/us/en/stores (last acc. July 3, 2023).
[10] *See* Vermont Secretary of State, "The Chill Foundation," available at https://bizfilings.vermont.gov/online/BusinessInquire/BusinessInformation?businessID=53934
[11] Joe Carberry, "Donna Carpenter Squashes Rumor That Burton Seeks $800 Million Sale," August 18, 2022, avail. at https://www.theinertia.com/mountain/donna-carpenter-squashes-rumor-that-burton-seeks-800-million-sale/ (last acc. July 3, 2023).
[12] *See* Vermont Secretary of State, "The Chill Foundation," available at https://bizfilings.vermont.gov/online/BusinessInquire/BusinessInformation?businessID=53934 (last acc. July 3, 2023).

exploration are then directly applied to everyday life, challenging youth to step out of their comfort zone – both on and off their board."[13]

21. Chill partners with "social service agencies, mental health agencies, foster care programs, juvenile justice programs, and schools in local communities to engage youth participants," and serves over 2,000 youth each year, and 30,000 since the program began.[14]

22. Defendant requires that its employees, and employees of Chill[15], provide Burton with their private, sensitive PII, including their names, dates of birth, Social Security numbers, driver's license numbers, as well as their government identification numbers, and financial account information, which Burton stores in its computer information technology systems.

23. In exchange for this information, Burton promises to safeguard employee PII, and to only use this confidential information for authorized purposes.

24. Defendant acknowledges the importance of properly safeguarding the private data and PII of individuals, including its employees, maintaining an online privacy policy, "Burton's Privacy and Cookies Policy," ("Privacy Policy").[16]

25. Burton's Privacy Policy states that, "How We Collect Personal Information," "From You: We collect personal information that you provide to us when you sign up for an account, contact us, make a purchase, enter a sweepstakes or contest, **or apply for a job with us**."[17]

26. Moreover, in its Privacy Policy, Defendant specifically states, promises, and

---

[13] Chill website, avail. at https://www.chill.org/programs/our-approach/ (last acc. July 3, 2023); https://www.chill.org/about-us/eligibility-requirements/ (last acc. July 3, 2023).
[14] Chill website, avail. at https://www.chill.org/about-us/ (last acc. July 3, 2023).
[15] Indeed, Burton solicits prospective employees of Chill through its own website. *See* https://www.burton.com/us/en/content/careers.html (last acc. Jul. 3, 2023).
[16] Burton's Privacy and Cookies Policy, Updated January 9, 2023, available at https://www.burton.com/us/en/help/privacy-na.html (last acc. Jul. 3, 2023), **attached as Exhibit 3.**
[17] *Id.* (emphasis added)

represents that it will protect the personal information, PII, it collects:

> **11. How Secure is My Personal Information?**
>
> We have implemented commercially reasonable precautions to protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, in accordance with industry practice and applicable laws. Please be aware that despite our best efforts, no data security measures can guarantee 100% security. While we strive to protect information transmitted on or through our site, we cannot and do not guarantee the security of any information you transmit on or through the site and you do so at your own risk.[18]

27. Further, Burton's Privacy Policy enumerates the purposes for which it may disclose the personal information and/or PII it collects, including as pertains to consumer transactions, to provide services, products, "[t]o enhance or customize your shopping experience with us," "[t]o better understand how users access and use our site, both on an aggregated and individualized basis," "[t]o evaluate our site and our offerings to you as a visitor," "[t]o respond to user preferences," "[f]or research and analytical purposes" "[t]o send you marketing notices including promotions of our products and services," and other purposes, none of which include the Data Breach.[19]

28. Except for the above purposes, Defendant promises and represents it "will keep all personal information collected from you, including personal information collected on burton.com, confidential."[20]

29. Plaintiff and the proposed Class Members, prospective, current, and former employees of Burton and Chill, would not have allowed their PII to be entrusted to Defendant had they known Burton would not adequately safeguard that information.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the

---

[18] *Id.*
[19] *Id.*
[20] *Id.*

proposed Class Members' PII, Defendant assumed legal and equitable duties to them, and knew or should have known that it was responsible for protecting their PII from unauthorized disclosure.

31. At all times Plaintiff and the members of the Proposed Class, have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiff and the proposed Class Members, relied on Defendant to keep their PII confidential and securely maintained.

B. Burton Fails to Adequately Safeguard PII—the Data Breach

32. Plaintiff and the proposed Class Members are current and former employees, and prospective employees of Burton and/or Chill, whose personal information, PII, was entrusted to Defendant.

33. Burton collected and maintained this PII in its computer information technology systems and networks.

34. On information and belief, from February 11, 2023 to March 9, 2023 the PII of Plaintiff and the proposed Class Members was unauthorizedly disclosed to third-party cybercriminals during an external system breach cyberattack, including their names, dates of birth, Social Security numbers, driver's license numbers or state issued identification number, passport number, and financial account information—the Data Breach.[21]

35. On or about February 14, 2023, Defendant posted a notice on its website, stating

---

[21] *See*: The Burton Corporation, Data Breach Notifications, Maine Attorney General, March 28, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/027f1a31-da35-49fe-a73f-10d0caeb5224.shtml (last acc. July 3, 2023); The Burton Corporation, Data Breach Notification to Maine Attorney General, including sample Notice, March 27, 2023, **("March 27, 2023 Data Breach Notice") attached as Exhibit 1;** The Burton Corporation, Data Breach Notifications, Maine Attorney General, May 26, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/74956a55-1020-4d9e-a3d6-0e9398870ebd.shtml (last acc. July 3, 2023); The Burton Corporation, Data Breach Notification to Maine Attorney General, including sample Notice, May 26, 2023, **("May 26, 2023 Data Breach Notice") attached as Exhibit 2.**

that "Burton recently experienced a cyber incident, which is impacting some of our operations. We are working closely with third-party specialists to investigate the incident and determine the full nature and scope. We are also making every effort to get our operations back up and running, but unfortunately are not able to process orders at this time."[22]

36. According to Defendant, following the Data Breach, Burton investigated the incident with the assistance of a third-party forensic specialist, evaluated the security of its systems, "reset relevant account passwords," reviewed the impacted files, and notified federal law enforcement.[23]

37. In addition, Burton implemented addition data security safeguards, as well as employee training, and reviewed its policies and procedures to prevent future data breaches.[24]

38. On or about March 27, 2023, Burton began sending written notice to Data Breach victims (March 27, 2023 Data Breach Notice, Exhibit 1), stating:

> On February 11, 2023, Burton discovered suspicious activity impacting the operability of certain systems. We quickly launched an investigation to determine the nature and scope of the activity, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed or taken by an unknown actor. We commenced a thorough review to determine whether sensitive information was present in the impacted files and folders. On March 9, 2023, it was determined that some of your information was present in the files and folders that may have been accessed or taken.[25]

39. In the March 27, 2023 Data Breach Notice, Burton admitted that victim's

---

[22] "Burton.com Update," Feb. 14, 2023, formerly available at https://www.burton.com/announcement/system-outage.html and now available via Wayback Machine at https://web.archive.org/web/20230217202057/https://www.burton.com/announcement/system-outage.html (last acc. Jul. 3, 2023).

[23] *See* **March 27, 2023 Data Breach Notice, Exhibit 1, sample Notice (Ex. A).**

[24] *See Id.*

[25] *See Id.*

information and PII were potentially accessed or taken by an unknown actor, including their names, dates of birth, Social Security numbers, driver's license numbers or state-issued identification numbers, passport numbers, and financial account information.[26]

40. Although Burton's March 27, 2023 Data Breach Notice attempted to minimize the harm caused by the Data Breach by qualifying that, "[t]o date, Burton has not received any reports of actual or attempted misuse of your information," therein Defendant encouraged affected persons to "remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring [their] free credit reports for suspicious activity and to detect errors," and apprised them of their ability to place a fraud alert on their credit files and a credit freeze on their credit reports.[27]

41. In addition, Burton offered victims of the Data Breach credit monitoring services through Experian's IdentityWorks for one (1) year.[28]

42. In the March 27, 2023 Data Breach Notice to affected persons, Burton obfuscated the nature of the Data Breach, failing to inform them how the breach had occurred, how long the their PII was accessible to unauthorized parties, or how many persons were impacted.

43. Indeed, on March 27, 2023, Burton reported the Data Breach to the Maine Attorney General, reporting that the Data Breach involved an "external system breach (hacking)" cyberattack, involving 737 people, and that the PII compromised included names and Social Security numbers.[29]

---

[26] *Id.*
[27] *Id.*
[28] *See Id.*
[29] *See* Maine Attorney General, Data Breach Notifications, March 27, 2023, avail. at https://apps.web.maine.gov/online/aeviewer/ME/40/027f1a31-da35-49fe-a73f-10d0caeb5224.shtml (last acc. Jul. 3, 2023).

44. In Burton's written notification to the Maine Attorney General, Exhibit 1, Defendant expounded that the Data Breach involved personal information of Chill's current and former employees.[30]

45. Subsequent to the foregoing, on or about May 26, 2023, Burton filed a supplemental report with the Maine Attorney General, stating that 5,282 individuals were affected in Defendant's February 11, 2023 Data Breach, *and* that Burton discovered the incident on April 7, 2023.[31]

46. On May 26, 2023, Burton began sending supplemental notices to the additional victims of the Data Breach (May 26, 2023 Data Breach Notice, Exhibit 2, Ex. A).

47. Defendant did not have adequate security protocols to prevent, detect, and stop the cybercriminals from executing the cyberattack on Burton's systems and accessing the voluminous PII of Plaintiff and the proposed Class Members which was stored therein in the Data Breach.

48. Further, Burton failed to adequately train its employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over individuals' PII in the Data Breach.

49. Defendant's tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed the data, meaning Burton had no effective means to detect and prevent attempted data breaches.

50. As a result of Burton's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social

---

[30] *See* **March 27, 2023 Data Breach Notice, Ex. 1, pg. 2.**

[31] See Data Breach Notifications, Maine Attorney General, May 26, 2023, available at https://apps.web.maine.gov/online/aeviewer/ME/40/74956a55-1020-4d9e-a3d6-0e9398870ebd.shtml (last acc. July 3, 2023); **May 26, 2023 Data Breach Notice, Exhibit 2.**

Security numbers. Accordingly, Burton's identity theft protection through Experian IdentityWorks for one (1) year is wholly insufficient to compensate Plaintiff and the Class Members for their damages caused by the Data Breach.

51. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered or will imminently injury and damages, including fraudulent misuse of PII, identity theft and fraudulent charges, forcing them to expend significant time and effort to remediate the consequences of the breach, as well as anxiety and emotional distress.

C. Plaintiff's Experience

52. From 2012 to 2014, to Plaintiff was an employee of Channel Island Surf Boards, owned by Burton from 2006[32] to 2020,[33] approximately, at its Carpinteria, California facility.

53. In connection with his application for employment and employment, Plaintiff was required to provide his PII to Burton which Defendant stored on its computer systems.

54. In late May 2023, Plaintiff received Burton's May 26, 2023 Data Breach Notice, in substantially the same format as Exhibit 2, Ex. A, informing him that his name, Social Security Number, and financial account information had been compromised in the Data Breach.

55. To his knowledge, Plaintiff has never been the victim of a prior data breach.

56. Given the nature of the Data Breach, on information and belief, Plaintiff's PII has been unauthorizedly disclosed to cybercriminals and is on the Dark Web for sale or to be utilized

---

[32] *See* Sarah Frahm, "Burton Aquires [sic] Channel Island Surfboards," OUTSIDE BUSINESS JOURNAL, June 30, 2006, avail. at https://www.outsidebusinessjournal.com/press-releases/burton-aquires-channel-island-surfboards/ (last acc. Jul. 3, 2023).

[33] *See* "Burton sells Channel Island Surfboardsm" December 1, 2020, Outdoor Industry Compass, avail. at https://www.oicompass.com/corporate-and-manda/burton-sells-channel-island-surfboards/85838.article

for fraudulent and criminal purposes.

57. As a direct result of the Data Breach, Plaintiff has suffered, or will imminently suffer, injury and damages, including the unauthorized disclosure of the PII itself, identity theft, fraudulent misuse of his PII, and fraudulent charges.

58. In addition, Plaintiff has spent time and effort attempting to remediate the harmful effects of the Data Breach, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

59. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

60. As a result of Burton's Data Breach, Plaintiff faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like his Social Security number.

D. This Data Breach was Foreseeable by Burton.

61. Plaintiff's and the proposed Class Members' PII was provided to Burton in connection with employment or applying for employment with Defendant, and with the reasonable expectation and mutual understanding that Burton would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

62. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and the Class Members from unauthorized disclosure. Defendant's

actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

63. Plaintiff and Class members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

64. According to the Identity Theft Resource Center's (ITRC) January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[34]

65. According to the ITRC's January 2023 report for 2022, "[t]he number of publicly reported data compromises in the U.S. totaled 1,802 in 2022. This represents the second highest number of data events in a single year and just 60 events short of matching 2021's all-time high number of data compromises."[35] In 2022, there were approximately 422 million individuals affected by cyberattacks.[36]

66. Moreover, of the 1,802 data breaches in 2022, ITRC reported that 1,560 involved compromised names, 1,143 involved compromised of Social Security Numbers, 633 involved compromised dates of birth, 499 involved compromised driver's license ID numbers, and 443

---

[34] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).

[35] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 7 (last acc. Jul. 3, 2023).

[36] *See Id.*, pg. 2.

involved bank account numbers—the types of PII unauthorized disclosed in this Data Breach.[37]

67. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Burton. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[38]

68. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

69. PII can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

70. Given the nature of the Data Breach, it was foreseeable that the compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. Burton Failed to Comply with FTC Guidelines

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

---

[37] *Id.*, pg. 6.
[38] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).

72. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[39]

73. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[40]

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[39] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[40] *See id.*

75. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

76. Burton failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

77. Defendant was at all times fully aware of its obligations to protect the PII of those individuals who were its employees or who applied for employment. Burton was also aware of the significant repercussions that would result from its failure to do so.

F. Burton Fails to Comply with Industry Standards

78. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

79. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security,

Incident Response Management, and Penetration Testing.[41]

80. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[42]

81. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports

---

[41] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. June 8, 2023).
[42] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[43]

82. Upon information and belief, Burton failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and the proposed Class Members' PII, resulting in the Data Breach.

G. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

83. Plaintiff and members of the proposed Class have suffered injury and damages from the misuse of their PII that can be directly traced to Burton, that has occurred, is ongoing, and/or imminently will occur.

84. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' PII, which is now been disclosed and is likely on

[43] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. June 8, 2023).

the Dark Web and being used for fraudulent purposes or sold for such purposes, causing widespread injury and damages.

85. The ramifications of Burton's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

86. Because Burton failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII;

b. The loss of the opportunity to control how PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

e. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Increase in spam texts and telephone calls;

i. Unauthorized use of stolen PII; and

j. The continued risk to their PII, which remains in the possession of Burton and is subject to further breaches so long as Burton fails to undertake the appropriate measures to protect the PII in its possession.

87. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

88. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[44]

89. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and

[44] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).

changing login information; contacting one of the credit bureaus to place a fraud alert on credit files (consider an extended fraud alert that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[45]

90. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

91. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

92. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

93. According to the Identity Theft Resource Center's 2022 Data Breach Report, "there has been a dramatic increase in identity scams and fraud where cybercriminals impersonate an individual using stolen data and/or information gleaned from social media accounts to apply for government benefits and to open new financial and non-financial accounts."[46] While this can mean that, "there are generally fewer victims of data breaches. [...] the financial impact is likely higher

---

[45] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last acc. June 8, 2023).

[46] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 8.

and the time to remediate the effects of the identity misuse is longer."[47]

94. Additionally, according to the ITRC, in 2022, "[d]ata breach notices suddenly lacked detail, resulting in increased risk for individuals and businesses as well as uncertainty about the true number of data breaches and victims."[48]

95. Further, according to the ITRC's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. 54% percent reported feelings of being violated.[49]

96. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII/PHI is a valuable property right.[50]

97. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII

---

[47] *Id.*
[48] *Id.*, pg. 8.
[49] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).
[50] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

has considerable market value.

98. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

99. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

100. Where the most PII belonging to Plaintiff and Class Members was accessible from Burton's network, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and the Class Members must vigilantly monitor their financial accounts for many years to come.

101. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[51]

102. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for

[51] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)

unemployment benefits, or apply for a job using a false identity.[52] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

103. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[53]

104. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[54]

102. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the criminal fraudulent activity, fraudulent charges, and attendant costs, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages

---

[52] *See id.*

[53] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[54] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 13, 2023).

as set forth in the preceding paragraphs.

103. Burton knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and strengthened its data systems accordingly.

CLASS ALLEGATIONS

114. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

115. Plaintiff brings this nationwide class action on behalf of himself, and on behalf of all other persons similarly situated, pursuant to Rule 23(a) of the Vermont Rules of Civil Procedure, and Vt. R. Civ. P. 23(b)(3).

116. Plaintiff proposes the following Class definition, subject to amendment based on information obtained through discovery:

> **All persons whose PII was compromised as a result of the Data Breach experienced by Defendant beginning on February 11, 2023 as announced by Burton, including all persons who received Defendant's Data Breach Notice.**

117. In addition, or in the alternative, Plaintiff proposes the following state class ("California Class") (together with the Nationwide Class, the "Class"):

> **California Class:**
>
> **All California residents whose PII was compromised as a result of the Data Breach experienced by Defendant beginning on February 11, 2023 as announced by Burton, including all persons who received Defendant's Data Breach Notice.**

118. Excluded from the Class are Defendant's officers, directors, any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

119. Plaintiff reserves the right to amend the definition of the Class or add a class or

subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

120. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

121. This action satisfies the requirements for a class action under Vt. R. Civ. P. 23(a)(1)-(4) and Vt. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

122. **Numerosity, Vt. R. Civ. P.(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the PII of approximately 5,282 individuals was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

123. **Commonality, Vt. R. Civ. P.(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data

Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether cybercriminals obtained Plaintiff's and Class Members' PII in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Burton failed to adequately respond to the Data Breach, including failing to timely notify the Plaintiff and the Class Members;

h. Whether Defendant's failures amounted to negligence;

i. Whether Plaintiff and the Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant was unjustly enriched;

k. Whether Defendant's acts violated the law, and;

l. Whether Plaintiff and the Class Members are entitled to damages including compensatory and punitive damages, and/or injunctive relief.

124. **Typicality, Vt. R. Civ. P.(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

125. **Adequacy, Vt. R. Civ. P.(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

126. **Predominance, Vt. R. Civ. P. (b)(3):** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data—PII—was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

127. **Superiority, Vt. R. Civ. P. (b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all

Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Burton's current and former employees and prospective employees, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

128. **Vt. R. Civ. P.(b)(2):** In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

129. Finally, all members of the proposed Class are readily ascertainable. Burton has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

130. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

131. Defendant collected and stored the PII of Plaintiff and the proposed Class Members as a condition of employment or as a condition of applying for employment with Defendant.

132. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiff and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

133. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their data in Defendant's possession.

134. By collecting and storing this data in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give

prompt notice to those affected in the case of a data breach.

135. Defendant owed a common law duty of care to Plaintiff and the Class Members to provide adequate data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

136. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

137. Defendant breached its duties, and was negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' PII;

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

138. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

139. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to them.

140. As a direct and proximate result of Defendant's negligence set forth in the preceding paragraphs, Plaintiff and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

141. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

142. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

143. Defendant had a duty to protect and maintain and provide adequate data security to maintain Plaintiff's and the Class Members' PII under Section 5 of the FTC Act, 15 U.S.C. § 45.

144. The FTC Act prohibits unfair business practices affecting commerce, which the

FTC has interpreted to include a failure to use reasonable measures to safeguard PII.

145. Defendant's violation of these duties is negligence *per se* under Vermont law.

146. Plaintiffs and the Class members are included in the class of persons that the FTC Act was intended to protect.

147. The harm the Data Breach caused is the type of harm the FTC Act was intended to guard against.

148. As a direct and proximate result of Defendant's negligence per se set forth in the preceding paragraphs, Plaintiff and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

149. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

150. Defendant offered to employ and/or accepted employment applications from Plaintiff and members of the Class in exchange for their PII.

151. In turn, through its conduct and representations, including but not limited to those outlined in its Privacy Policy and other policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons, and promised it would safeguard employee and applicant PII.

152. Plaintiff and the Class Members accepted Defendant's offer by providing PII to Defendant in exchange for employment or to apply with Defendant.

153. Implicit in the parties' agreement was that Defendant would provide protect Plaintiff's and the Class Members' PII, and would provide them with prompt and adequate notice of all unauthorized access and/or theft of their PII.

154. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such agreement with Burton.

155. The protection of Plaintiff's and Class Members' PII was a material aspect of these implied contracts.

156. Defendant materially breached the contracts it had entered with Plaintiffs and Class Members by failing to safeguard such information and failing to notify them promptly of Data Breach that compromised such information, including failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

157. As a direct and proximate result of Defendant's breach of implied contract set forth in the preceding paragraphs, Plaintiff and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach.

158. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

159. Plaintiffs and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

160. The covenant of good faith and fair dealing is an element of every contract under Vermont law. All such contracts impose upon each party a duty of good faith and fair dealing. It is an implied promise that protects against conduct that violates community standards of decency, fairness or reasonableness. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

161. In failing to adequately protect current and former employee PII and applicant PII, and in failing to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently. Defendant violated its duty of good faith and fair dealing.

162. Plaintiff and Class Members have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

163. Plaintiff and the Class Members are entitled to compensatory and consequential damages suffered as a result of Defendant's breach of implied contract including the covenant of good faith and fair dealing.

164. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

165. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

166. This claim for Unjust Enrichment is brought in the alternate to the claim for Breach of Implied Contract (Count III).

167. Plaintiff and proposed Class Members conferred benefits upon Defendant in the form of services through employment, and in the form of valuable PII entrusted to Defendant.

168. Defendant appreciated or knew of these benefits that it received, as required to facilitate employment and applications for employment. And under principles of equity and good conscience, this court should not allow Defendant to retain the full value of these benefits—specifically, the value of services and PII of Plaintiff and Class Members.

169. After all, Defendant failed to adequately protect Plaintiff's and Class Members' PII. And if such inadequacies were known, then Plaintiff and the members of the Class would never have rendered services in connection with employment to Defendant, nor disclosed their PII.

170. As a direct and proximate result of Defendant's unjust enrichment set forth in the preceding paragraphs, Plaintiff and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

171. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—the value of all services and benefits that were unlawfully or

inequitably gained despite Defendant's misconduct and the resulting Data Breach.

COUNT V
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

172. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

173. Vermont recognizes the tort of invasion of privacy by intrusion upon seclusion.

174. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

175. Defendant owed a duty to Plaintiff and the Class Members, to keep their PII confidential.

176. Defendant failed to protect said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons, which is now publicly available, and on information and belief, on the dark web, and subject to fraudulent misuse.

177. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII.

178. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

179. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff's and the Class Members' PII was disclosed to Defendant in connection with employment and/or application for employment with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

180. The Data Breach constitutes an intentional or reckless, and substantial, interference by Defendant with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

181. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its data security practices were inadequate and insufficient.

182. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PII.

183. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

184. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

185. As a direct and proximate result of Defendant's invasion of privacy, intrusion upon seclusion, set forth in the preceding paragraphs, Plaintiff and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

186. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

187. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT VI
VIOLATION OF THE VERMONT CONSUMER PROTECTION ACT,
9 V.S.A. § 2453, *ET SEQ.*
(On Behalf of Plaintiff and the Class)

188. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

189. Defendant committed unfair or deceptive acts within the meaning of the Vermont Consumer Protection Act, 9 V.S.A. § 2453.

190. Specifically, Defendant committed acts that misrepresented that its services had characteristics, benefits, and qualities that they did not have, and omitted critical details regarding its data security. These acts misled consumers into thinking their PII was safe. These acts include, but are not limited to:

a. Defendant failed to enact adequate privacy and security measures to protect Plaintiff's and Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Defendant failed to take proper action following known security risks;

c. Defendant knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Plaintiff's and Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Plaintiff's and Class Members' PII;

e. Defendant knowingly and fraudulently misrepresented that it would comply with the requirements of relevant laws pertaining to the privacy and security of Plaintiff's and Class Members' PII; and,

f. Defendant failed to maintain the privacy and security of Class Members' PII, in violation of duties imposed by applicable law, including but not limited to the Vermont Security Breach Notice Act, 9 V.S.A. § 2435, directly and proximately causing the Data Breach.

191. As a direct and proximate result of Defendant's above deceptive trade practices, Plaintiff and Class Members have suffered or will imminently suffer injury and damages as set forth herein, including fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and the value of time and labor expended to mitigate the consequences of the Data Breach, and are entitled to compensatory, actual, and punitive damages as a result.

192. Plaintiff and Class Members seek all available relief under 9 V.S.A. § 2461, including, but not limited to, actual damages; restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

COUNT VII
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018
Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiff and the Class or alternatively the California Class)

193. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

194. This claim is pleaded on behalf of Plaintiff and the Class, or alternatively, the California Class.

195. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

196. As a result, in 2018, the California Legislature passed the California Consumer Privacy Act of 2018 ("CCPA"), giving consumers broad protections and rights intended to safeguard their personal information.

197. Among other things, the CCPA, Cal. Civ. Code §§ 1798.100(e), imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

198. On information and belief, Burton is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

199. Section 1798.150(a)(1) of the CCPA provides: "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to

the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

200. Through the above-detailed conduct, Defendant violated the CCPA by subjecting the nonencrypted and nonredacted PII of Plaintiff and Class Members to unauthorized access and exfiltration, theft, or disclosure as a result of Burton's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

201. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because he is natural person residing in the state of California.

202. On information and belief, Defendant is a "business" as defined by Civ. Code § 1798.140(c) because it does business in the state of California and has annual revenues of in excess of $25,000,000.

203. The CCPA provides that "personal information" includes "[i]dentifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers." *See* Civ. Code § 1798.140.

204. Plaintiff's and the Class's or California Class's PII compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

205. Through the Data Breach, Plaintiff's PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

206. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

207. Concurrent with the filing of this Complaint, Plaintiff provides notice by letter to Defendant pursuant to Cal. Civ. Code § 1798.150(b) identifying the specific provisions of the CCPA Plaintiff alleges Defendant has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Defendant is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

COUNT VIII
VIOLATION OF CALIFORNIA'S CONSUMER RECORDS
Cal. Civ. Code §§ 1798.82, *et seq.* ("CCRA")
(On Behalf of Plaintiff and the Class or alternatively the California Class)

208. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

209. This claim is pleaded on behalf of Plaintiff and the Class, or alternatively, the California Class.

210. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under Section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay…"

211. The CCRA further provides: "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data *immediately* following discovery, if the personal information was, or is reasonably believed to have been, acquired by an

unauthorized person." Cal. Civ. Code § 1798.82(b) (emphasis added).

212. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
>
> (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

Cal. Civ. Code § 1798.82(d)(2).

213. The Data Breach described herein constitutes a "breach of the security system" of Defendant.

214. As alleged herein, it took *months* from when Defendant first identified the Data Breach in February 2023, *or* on or about March 9, 2023, for Defendant to begin informing Plaintiff and the Class or California Class Members about the Data Breach. Burton unreasonably delayed information to Plaintiff and Class Members about the Data Breach, affecting their PII, after Defendant knew the Data Breach had occurred; and, indeed, Defendant changed the date of

discovery of the Data Breach to April 7, 2023 in the May 26, 2023 Data Breach Notice, Ex. 2.

215. Defendant failed to disclose to Plaintiff and California Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII, when Burton knew or reasonably believed such information had been compromised.

216. Defendant's ongoing business interests gave Burton incentive to conceal the Data Breach from the public to ensure continued revenue.

217. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and California Class Members would impede its investigation.

218. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and the California Class Members or Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their PII would have had less value to identity thieves.

219. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and the California Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

220. Plaintiff and California Class Members or Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to, to the damages suffered by Plaintiff and Class Members as alleged above and equitable relief.

221. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to Burton conducted with

the intent on the part of Defendant depriving Plaintiff and Class Members of "legal rights or otherwise causing injury."

222. In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c) in that it was despicable conduct carried on by Burton with a willful and conscious disregard of the rights or safety of Plaintiff and Class Members and despicable conduct that has subjected Plaintiff and Class Members to cruel and unjust hardship in conscious disregard of their rights.

223. As a result, Plaintiff and Class Members are entitled to punitive damages under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, DAVID MORGAN, on behalf of himself, and all others similarly situated, prays for judgment as follows:

A. Trial by jury pursuant to on all claims so triable;

B. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

C. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and statutory damages, and punitive damages, as allowed by law;

D. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and

the Class;

G. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiff and the Class are entitled.

Dated: July 19, 2023

Respectfully submitted,

D. James Mackall
SHILLEN MACKALL & SELDON
21710 Maxham Meadow Way, Suite 2A
Woodstock, Vermont 05091
(802) 243-0078
djmackall@promotingjustice.com

Lynn A. Toops*
Mary Kate Dugan*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV *
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss*
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com

*Motion for *Pro Hac Vice* Admission forthcoming

Counsel for Plaintiff and the Proposed Class

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, The Burton Corporation ("Burton") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about February 11, 2023, Burton experienced a disruption to certain computer systems following a sophisticated cyber-attack. Burton quickly launched an investigation to determine the nature and scope of the activity, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed or taken by an unknown actor. Burton commenced a thorough review to determine whether sensitive information was present in the impacted files and folders. On March 9, 2023, it was determined that some information related to Maine residents was present in the files and folders that may have been accessed or taken.

Burton collects data from The Chill Foundation ("Chill"), a 501(c)(3) nonprofit organization that is located on Burton's campus at 180 Queen City Park Road, Burlington, Vermont 05401. The investigation determined that personal information related to current or former employees of Chill was also potentially accessed or taken by an unknown actor. Burton notified Chill of this event and is notifying Chill employees if it determined that their personal information was impacted.

While the information varies for each individual, the information that could have been subject to unauthorized access includes name, date of birth, Social Security number, driver's license number or state-issued identification number, passport number, and financial account information.

Notice to Maine Residents

On or about March 27, 2023, Burton began providing written notice of this incident to seven (7) Maine residents. Six (6) Maine residents are current or former employees of Burton, and one (1) Maine resident is a current or former employee of Chill. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Burton's investigation into this event is ongoing. Burton may supplement this notification if it is determined that a significant number of additional Maine residents were impacted by this event.

Other Steps Taken and To Be Taken

Upon discovering the event, Burton moved quickly to investigate and respond to the incident, assess the security of Burton systems, and reset relevant account passwords. Burton also began reviewing the contents of impacted systems to determine whether they contained personal information in order to identify potentially affected individuals. Further, Burton notified federal law enforcement regarding the event. Burton is also working to implement additional safeguards and training to its employees and is reviewing existing policies and procedures to reduce the likelihood of a similar future incident. Burton is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Burton is also notifying relevant state regulators, as required.

Additionally, Burton is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Burton is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

BURTON

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 27, 2023

J2086-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF [Extra2]

Dear Sample A. Sample:

The Burton Corporation ("Burton") writes to inform you of an incident that may affect the security of some of your information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On February 11, 2023, Burton discovered suspicious activity impacting the operability of certain systems. We quickly launched an investigation to determine the nature and scope of the activity, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed or taken by an unknown actor. We commenced a thorough review to determine whether sensitive information was present in the impacted files and folders. On March 9, 2023, it was determined that some of your information was present in the files and folders that may have been accessed or taken.

What Information Was Involved? Burton is notifying you out of an abundance of caution because information related to you was identified in the files that were potentially accessed or taken by an unknown actor. The information related to you that was potentially accessible may include your name, date of birth, Social Security number, driver's license number or state-issued identification number, passport number, and financial account information. To date, Burton has not received any reports of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to the incident, assess the security of relevant systems, and reset relevant account passwords. We are also reviewing the contents of the impacted systems to determine whether they contained personal information, reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals, and notifying potentially affected individuals. As part of our ongoing commitment to the security of information, we are also reviewing existing policies and procedures to reduce the likelihood of a similar future incident. Burton is also notifying relevant state and federal regulators, as required. Finally, we reported this incident to law enforcement, and will participate with any criminal investigation into this matter.

As an added precaution, we are also offering complimentary access to Experian's® IdentityWorks℠ for [Extra3] months. These services include identity theft detection and resolution services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information.* There, you will also find more information on the identity theft detection and resolution services we are making available to you, and how to enroll.

000000

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-833-420-2847 Monday – Friday, 9 am to 11 pm ET; Saturday – Sunday, 11 am to 8 pm ET.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

John Lacy
Chief Executive Officer
The Burton Corporation

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring and Resolution Services

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **June 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-420-2847 by June 30, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft

should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Burton is located at 180 Queen City Park Road, Burlington, Vermont, 05401.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 7 Rhode Island residents impacted by this incident.

EXHIBIT 1

This notice supplements our previous notice dated March 28, 2023. Our prior submission is attached hereto as ***Exhibit AA***. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, The Burton Corporation ("Burton") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about February 11, 2023, Burton experienced a disruption to certain computer systems following a sophisticated cyber-attack. Burton quickly launched an investigation to determine the nature and scope of the activity, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed or taken by an unknown actor. Burton commenced a thorough review to determine whether sensitive information was present in the impacted files and folders.

As stated in our previous notice, Burton collects data from The Chill Foundation ("Chill"), a 501(c)(3) nonprofit organization that is located on Burton's campus at 180 Queen City Park Road, Burlington, Vermont 05401. The investigation determined that personal information related to current or former employees of Chill, as well as dependents and beneficiaries, was also potentially accessed or taken by an unknown actor. Burton notified Chill of this event and is notifying impacted individuals associated with Chill if it determined that their personal information was impacted.

Since notifying your office on March 28, 2023, Burton provided written notice of this incident to forty-five (45) additional Maine residents whose information was present in the files and folders that may have been accessed or taken. Forty-one (41) Maine residents are related to Burton, and four (4) Maine residents are related to Chill.

While the information varies for each individual, the information that could have been subject to unauthorized access for these additional Maine residents includes name, date of birth, Social Security number, driver's license number or state-issued identification number, passport number, and financial account information.

Notice to Maine Residents

On or about May 5, 2023 and May 26, 2023, Burton provided written notice of this incident to the additional forty-five (45) Maine residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***. Burton's investigation into this event is ongoing. Burton may supplement this notification if it is determined that a significant number of additional Maine residents were impacted by this event.

Other Steps Taken and To Be Taken

Upon discovering the event, Burton moved quickly to investigate and respond to the incident, assess the security of Burton systems, and reset relevant account passwords. Burton also began reviewing the contents of impacted systems to determine whether they contained personal information in order to identify potentially affected individuals. Further, Burton notified federal law enforcement regarding the event. Burton is also working to implement additional safeguards and training to its employees and is reviewing existing policies and procedures to reduce the likelihood of a similar future incident. Burton is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Burton is also notifying relevant state regulators, as required.

Additionally, Burton is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Burton is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT AA

OFFICE OF THE
Maine Attorney General

Maine Security Breach Reporting Form - Review

EDIT

Type of Organization (Please select one)	Other Commercial
Entity Name	The Burton Corporation
Street Address	180 Queen City Park Road
City	Burlington
State, or Country if outside the US	Vermont
Zip Code	05401
Name	Andrew McConnell
Title	Chief Financial Officer
Telephone Number	8026603235
Email Address	andrewm@burton.com
Relationship to entity whose information was compromised	Chief Financial Officer
Total number of persons affected (including Maine residents)	737
Total number of Maine residents affected	7
Date(s) Breach Occurred	02/11/2023
Date Breach Discovered	03/09/2023
Description of the Breach (please check all that apply)	External system breach (hacking)
Information Acquired - Name or other personal identifier in combination with (please check all that apply)	Social Security Number Driver's License Number or Non-Driver Identification Card Number Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)
Type of notification	Written
Date(s) of consumer notification	03/27/2023
Were identity theft protection services offered?	Yes
If yes, please provide the duration, the provider of the	12 months, Experian, credit monitoring and identity restoration

service and a brief description of the service

Disclosure and Agreement

By checking the box below, you certify that all information supplied on this form is true and accurate to the best of your knowledge.

The disclosure statement has been read and agreed to by the individual submitting this Maine Attorney General Reporting Form. *

Michele Veltri

PREVIOUS CONTINUE TO SUBMIT FORM

OFFICE OF THE
Maine Attorney General

Maine Security Breach Reporting Form

Thank you for submitting the breach details through this reporting form. The information you have provided has been submitted to the agency.

Please close this browser window.

< PREVIOUS FINISH

EXHIBIT 1

To the March 28, 2023 Notice

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, The Burton Corporation ("Burton") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about February 11, 2023, Burton experienced a disruption to certain computer systems following a sophisticated cyber-attack. Burton quickly launched an investigation to determine the nature and scope of the activity, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed or taken by an unknown actor. Burton commenced a thorough review to determine whether sensitive information was present in the impacted files and folders. On March 9, 2023, it was determined that some information related to Maine residents was present in the files and folders that may have been accessed or taken.

Burton collects data from The Chill Foundation ("Chill"), a 501(c)(3) nonprofit organization that is located on Burton's campus at 180 Queen City Park Road, Burlington, Vermont 05401. The investigation determined that personal information related to current or former employees of Chill was also potentially accessed or taken by an unknown actor. Burton notified Chill of this event and is notifying Chill employees if it determined that their personal information was impacted.

While the information varies for each individual, the information that could have been subject to unauthorized access includes name, date of birth, Social Security number, driver's license number or state-issued identification number, passport number, and financial account information.

Notice to Maine Residents

On or about March 27, 2023, Burton began providing written notice of this incident to seven (7) Maine residents. Six (6) Maine residents are current or former employees of Burton, and one (1) Maine resident is a current or former employee of Chill. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Burton's investigation into this event is ongoing. Burton may supplement this notification if it is determined that a significant number of additional Maine residents were impacted by this event.

Other Steps Taken and To Be Taken

Upon discovering the event, Burton moved quickly to investigate and respond to the incident, assess the security of Burton systems, and reset relevant account passwords. Burton also began reviewing the contents of impacted systems to determine whether they contained personal information in order to identify potentially affected individuals. Further, Burton notified federal law enforcement regarding the event. Burton is also working to implement additional safeguards and training to its employees and is reviewing existing policies and procedures to reduce the likelihood of a similar future incident. Burton is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Burton is also notifying relevant state regulators, as required.

Additionally, Burton is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Burton is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

BURTON

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 26, 2023

J4834-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF [Extra1]

Dear Sample A. Sample:

The Burton Corporation ("Burton") writes to inform you of an incident that may affect the security of some of your information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On February 11, 2023, Burton discovered suspicious activity impacting the operability of certain systems. We quickly launched an investigation to determine the nature and scope of the activity, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed or taken by an unknown actor. We commenced a thorough review to determine whether sensitive information was present in the impacted files and folders. On April 7, 2023, it was determined that some of your information was present in the files and folders that may have been accessed or taken. We then commenced an advanced address lookup service in order to identify the most recent contact information for affected individuals.

What Information Was Involved? Burton is notifying you out of an abundance of caution because information related to you was identified in the files that were potentially accessed or taken by an unknown actor. The information related to you that was potentially accessible may include your name, Social Security number, and financial account information. To date, Burton has not received any reports of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to the incident, assess the security of relevant systems, and reset relevant account passwords. We are also reviewing the contents of the impacted systems to determine whether they contained personal information, reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals, and notifying potentially affected individuals. As part of our ongoing commitment to the security of information, we are also reviewing existing policies and procedures to reduce the likelihood of a similar future incident. Burton is also notifying relevant state and federal regulators, as required. Finally, we reported this incident to law enforcement, and will participate with any criminal investigation into this matter.

As an added precaution, we are also offering complimentary access to Experian's® IdentityWorks℠ for ## months. These services include identity theft detection and resolution services.

000000

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information.* There, you will also find more information on the identity theft detection and resolution services we are making available to you, and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-833-420-2847 Monday – Friday, 9 am to 11 pm ET; Saturday – Sunday, 11 am to 8 pm ET.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

John Lacy
Chief Executive Officer
The Burton Corporation

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring and Resolution Services

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **August 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-420-2847 by August 31, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft

should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Burton is located at 180 Queen City Park Road, Burlington, Vermont, 05401.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 25 Rhode Island residents impacted by this incident.

BURTON'S PRIVACY AND COOKIES POLICY

Updated January 9, 2023

This notice describes Burton's Privacy Policy. By visiting burton.com, you consent to the practices described in this Privacy Policy. Burton may modify this Privacy Policy at any time. Your continued use of Burton's products and services and burton.com constitutes your acceptance of this Privacy Policy and any updates. This Privacy Policy is incorporated into, and is subject to, Burton's Terms of Use.

For the purposes of European data protection law, the data controller of burton.com is The Burton Corporation. The data controller is responsible for determining why your data is collected and how it is processed.

In this Policy, we cover:

- Notice at Collection
- Information We Collect
- How We Collect Information
- How We Use Your Information
- Who We Share Information With
- Google Analytics
- Protection of Children's Privacy
- Your Rights
- Important Information for U.S. Residents of California
- Information for International Users
- How Secure is My Personal Information?

act Us

1. Notice at Collection

Personal Information We Collect	How We Use Your Personal Information
Contact Information	• To fulfill the services and provide the products you request from us • To better understand how users access and use site, both on an aggregated and individualized basis • To respond to user preferences • For research and analytical purposes • To advertise and market our products and services
Account Information	• To fulfill the services and provide the products you request from us • To enhance or customize your shopping experience with us • To better understand how users access and use site, both on an aggregated and individualized basis • To respond to user preferences • For research and analytical purposes • To advertise and market our products and services
Demographic Information	• To enhance or customize your shopping experience with us • To better understand how users access and use site, both on an aggregated and individualized basis • For research and analytical purposes • To advertise and market our products and services
Payment Information	• To fulfill the services and provide the products you request from us

	• To better understand how users access and use site, both on an aggregated and individualized basis • For research and analytical purposes
Commercial or Transactions Information	• To fulfill the services and provide the products you request from us • To better understand how users access and use site, both on an aggregated and individualized basis • For research and analytical purposes • To advertise and market our products and services
Precise Location Information	• To fulfill the services and provide the products you request from us • To better understand how users access and use site, both on an aggregated and individualized basis • For research and analytical purposes
Social Media Information	• To better understand how users access and use site, both on an aggregated and individualized basis. • For research and analytical purposes • To advertise and market our products and services
Internet Activity Information	• To fulfill the services and provide the products you request from us • To enhance or customize your shopping experience with us • To better understand how users access and use site, both on an aggregated and individualized basis • To evaluate our site and our offerings to you as a visitor • To respond to user preferences

	• For research and analytical purposes • To advertise and market our products and services
Information About Your Customer Experience	• To better understand how users access and use site, both on an aggregated and individualized basis • For research and analytical purposes • To advertise and market our products and services
Inferences	• To understand more about you and your preferences so that we can improve and customize our products and services • For research and analytical purposes • To advertise and market our products and services

We may sell or share Contact Information, Account Information, Demographic Information, Social Media Information, Internet Activity Information, Information About Your Customer Experience, and inferences we may make about you to third parties for targeted advertising on and off burton.com , to measure the effectiveness of our advertising and prevent fraud, and to assist us in providing you with products and services.

We will retain your information for as long as reasonably necessary for the purposes described above.

To learn how you can exercise your rights in relation to your personal information, under the laws of certain states, including California please visit this link.

2. Personal Information We Collect

We collect information you give us, permit us to access or when you enter into a contract or sales transaction with us. Such information generally falls into the following categories:

- **Contact information**, including identifiers such as your name, e-mail, physical address and telephone number;
- **Account information**, such as your username and password, birthdate, order history and preferences when using our products or services and information we need to honor warranties for products you have purchased;

- **Demographic information**, such as your gender and your date of birth;
- **Payment information**, such as your credit card number, expiration date, card verification number, and billing address if you make a purchase.
- **Commercial or transactions information**, including records of products and services purchased, obtained, or considered, and your engagement with our site and services.
- **Precise location information**, including GPS information, activity and performance information;
- **Social media information**, including any profile information and contact lists (collected in limited circumstances); and
- **Internet activity information**, such as your IP address, browser type and language, operating system, cookie information (described below), web beacons (described below), pages visited on our site, referring and exit pages, and the dates and times of the visits.
- **Information about your customer experience**, including your responses to survey questions, reviews and other feedback you provide, and general information that customers provide about customers' experiences. Our methods for collecting information about your experience may also collect information about your browser or device, but generally do not include identifying information such as your name and email address, unless you choose to provide it.
- **Inferences** about you and your interests and personal preferences (such as the sports and activities that may interest you.

We process your personal information on the basis that your personal information is required for us to provide the website, products and services to you under the relevant contract between us.

3. How We Collect Personal Information

We collect and obtain personal information:

- **From you**. We collect personal information that you provide to us when you sign up for an account, contact us, make a purchase, enter a sweepstakes or contest, or apply for a job with us.
- **From your device**, including through:
    - Cookies. We automatically collect information using "cookies." Cookies are small data files stored on your hard drive by a web site. Among other things, cookies help us improve our site and your experience. Using cookies helps us see which areas and features are popular and helps us count visits to our site. In certain jurisdictions, you may be asked to consent to any cookies that are not deemed "necessary" to the operation of our website. In that case, when you click "Accept" on our consent request, you agree to the placement of cookies on your browser by us, our analytics and service providers, and marketing

partners. If you do not click "Accept", then we will remember your opt-out preference. You may change your preferences or withdraw your consent at any time. Many web browsers are set to accept cookies by default. Wherever you are located, y you can usually choose to set your browser to remove cookies and to reject cookies from our site. If you set your browser not to accept cookies or if you reject a cookie, it may affect certain features or services of our site.

- Web Beacons. We collect information using web beacons. Web beacons, or "gifs," are electronic images that are used on our site or in our e-mails. We use web beacons to deliver cookies, count visits, understand usage and campaign effectiveness and to tell if an email has been opened and acted upon. If you do not wish for us to track emails we send you, some e-mail services allow you to adjust your display to turn off HTML or images which may disable tracking, or you may unsubscribe from our marketing e-mails via contacting Burton's Rider Services or clicking "unsubscribe" in any marketing email.

- **From other third parties**. A number of our suppliers also set cookies, web beacons, pixels, tags, and scripts on your browser or device on our behalf when you visit our site in order to deliver the services they are providing, analyze trends and site performance, administer the site, track users' movements and behavior around the site, measure advertising effectiveness, and prevent fraud. This means that when you visit our site you receive cookies from third party websites or domains. We receive reports based on the use of these technologies by these companies on an individual and aggregated basis. In addition, we may receive your information from third-party shopping services. We use that information only to fulfill orders.

In the U.S., you can opt out of third-party tracking on our website or others for online behavioral advertising by visiting the Digital Advertising Alliance's (DAA's) Consumer Choice page at http://www.aboutads.info/choices/ or the Network Advertising Initiative's page at http://www.networkadvertising.org/choices/. In Europe, you can make choices about whether to allow tracking when you first visit our site and are asked to accept cookies and other trackers.

In some U.S. states, you may choose not to have your personal information sold, shared, or disclosed through cookies or otherwise. See "Your U.S. State Privacy Rights" for more details on how you can make these choices in California and certain other states.

4. How We Use Your Personal Information

Except as set forth below in this section, we will keep all personal information collected from you, including personal information collected on burton.com, confidential. We will use the collected personal information for the following legitimate purposes:

- **To fulfill the services and provide the products you request from us.** For this purpose, we typically collect contact information, account information, payment information, commercial or transactions information, location information, and internet activity information.
- **To enhance or customize your shopping experience with us.** For this purpose, we typically use account information, demographic information, and internet activity information.
- **To better understand how users access and use our site, both on an aggregated and individualized basis.** For this purpose, we typically use all categories of personal information that we collect.
- **To evaluate our site and our offerings to you as a visitor.** For this purpose, we typically use internet activity information.
- **To respond to user preferences.** For this purpose, we typically use account information, contact information, and internet activity information.
- **For research and analytical purposes.** For this purpose, we typically use all categories of information that we collect.
- **To send you marketing notices including promotions of our products and services.** For this purpose, we typically use contact information, demographic information, and location information.

We use sensitive personal information only for the purposes permitted under California law or regulations.

5. Disclosure of Personal Information

We disclose your personal information as described below:

- **Authorized service providers.** We employ other companies to perform functions on our behalf. These other companies help us by fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, analyzing traffic on our websites, providing marketing assistance, providing surveys about our products and services, providing search results and links (including paid listings and links), processing credit card payments, assessing risk, automating decisions, and preventing fraud, and providing customer service. These companies have access to your information only as needed to perform their functions, but they are not permitted to use it for other purposes. We disclose account information, payment information, and commercial information to these service providers. We may also disclose information about your customer experience with service providers who help us work to improve your experience. We may provide location information and Internet activity information to service providers in certain circumstances.
- **Advertising platforms and social networks.** We disclose information to companies that help us with our advertising and marketing efforts, including advertising

platforms and social networks. For example, we disclose Internet activity data and email addresses or other contact information to advertising platforms and social networks when we advertise through their platforms.

- **Data partners.** In the United States, we participate in cooperative data sharing programs for marketing purposes, where participants provide customer contact information for U.S. customers and commercial/transactions information to the program vendor. We provide account information and Internet activity information to these data partners. This disclosure of information allows participants to identify and segment persons who may be interested in the participants' products and services in order to target such persons with relevant marketing. In connection with our participation in these programs, we disclose U.S. customers' names, physical addresses, aggregate transaction information, and purchase history information to other companies for their marketing purposes. (We do not generally disclose names and addresses to social networks.) If you are a U.S. customer and you do not wish to have your name, physical address, transaction or purchase history information disclosed or used through these cooperative programs, you may choose to not participate and can let us know by contacting us via the methods set forth on https://www.burton.com/us/en/contact-us.
- **Burton companies.** We disclose your information to our affiliate companies in order to perform our contract with you, including the provision of our products and services. We disclose all categories of information freely to our affiliated companies.
- **Law enforcement agencies, governmental authorities or regulators.** We release account and other personal information when we believe release is appropriate to comply with the law, enforce or apply our conditions of use and other agreements, or protect the rights, property, or safety of burton.com, our users, or others. Typically, government authorities request account information, but we disclose any information required by valid legal process.
- **Credit reference and fraud prevention agencies.** We exchange information with other companies and organizations for fraud protection and credit risk reduction. We disclose account information, including payment information and sometimes Internet activity information to these companies.
- **Organizations in connection with a business transfer.** We will release information if we are acquired by or merged with another company, or if substantially all of our assets are transferred to another company, or as part of a bankruptcy proceeding.

Otherwise, we will keep the information we hold about you for as long as we believe is necessary to provide you the products, information and services you requested or as reasonably use for commercial purposes unless you tell us you want us to stop holding the information. We retain behavior information collected through Google Analytics for a period of 50 months and delete such information at the end of this period.

6. Google Analytics

Burton.com uses a tool called Google Analytics for site analysis and also makes use of other Google Analytics features, including remarketing and audiences. For more information about Google Analytics and these features, go to http://www.google.com/policies/privacy/partners ("How Google uses data when you use our partners' sites or apps"). Website users who don't want their data collected and disclosed to Google Analytics can install the Google Analytics opt-out browser add-on. To opt out of Google Analytics, go to https://tools.google.com/dlpage/gaoptout.

7. Protection of Children's Privacy

We do not solicit or knowingly collect any personal information from children under the age of 18, and do not knowingly sell or share the personal information of anyone under the age of 16. This website is intended for users over the age of 18.. If you believe that a child under 13 may have provided personal information to us, please contact us at support.na@burton.com

8. Your Rights and Choices

We collect and process your personal information on the basis that your personal information is required for us to provide the website, and any products and services you request or for the legitimate purposes set out in this Policy. In accordance with applicable law, you may have the right to request that we:

- provide you information about how we use your personal information;
- give you access to, and a copy of, your personal information that we store on our system;
- update, correct or delete your information held in our files;
- stop using, and require that third parties stop using, some or all of your personal information for certain purposes, even if you continue to use our site or services; and
- discontinue contacting you.

If you would like to make a request, you can send us an email at support.na@burton.com or contact us by mail at: The Burton Corporation, 180 Queen City Park Road, Burlington, VT 05401, Attn: General Counsel.

Additionally, if you are located in the European Union, you have the right to lodge a complaint with your local supervisory data protection authority about our use of your personal information.

9. Important Information for U.S. Residents

If you are resident of certain states in the U.S., you may have additional choices and rights regarding your personal information. Some of these choices and rights vary based on where you live. For additional information about your choices and rights under certain U S. state privacy laws, please visit this link.

10. Information for International Users

Our digital operations are conducted, in whole or in part, in the United States, which means that your information is transferred from your region and transferred to, processed and stored in the United States. The information is also transferred from the United States to your region for payment processing, warehousing and shipping purposes pursuant to our contractual agreements with such regional processors, warehouses and shippers. Regardless of where you live, you understand and agree that when you provide data to us for us to process in accordance with our legitimate interests or to fulfill an agreement with you (for example when you make a purchase) your data will be transferred, processed and stored in the United States, and you will allow Burton to use and collect your personal information in accordance with this Privacy Policy. When another company transfers your data to the U.S., we agree to protect your data as required under the EU General Data Protection Regulation.

11. How Secure is My Personal Information?

We have implemented commercially reasonable precautions to protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, in accordance with industry practice and applicable laws. Please be aware that despite our best efforts, no data security measures can guarantee 100% security. While we strive to protect information transmitted on or through our site, we cannot and do not guarantee the security of any information you transmit on or through the site and you do so at your own risk.

You should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared computer, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity, except where otherwise required by applicable law.

12. Questions/Contact Us

If you have questions about the guidelines described in this Privacy Policy, please email us directly at support.na@burton.com.